

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri**FILED**

JUN 29 2021

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

THE PREMISES LOCATED AT: 507 E Missouri St, Kirksville,
MO 63501 located in the Eastern District of Missouri. This
premises is further identified in Attachment A.

Case No. 4:21 MJ 5163 NAB

Signed and Submitted to the Court for Filing by
Reliable Electronic Means

APPLICATION FOR A SEARCH WARRANT

I, S/A Thomas Putting, a federal law enforcement officer or an attorney for the government
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A.

located in the EASTERN District of MISSOURI, there is now concealed

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. Section 2252A(a)(1)
18 U.S.C. 2252A(a)(5)(B)


Offense Description

Distribution of Child Pornography
Possession of Child Pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

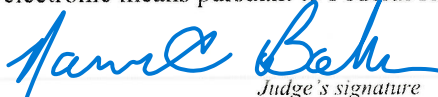

 Applicant's signature
 Special Agent Thomas Putting, Homeland Security
 Investigations

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal
Procedures 4.1 and 4.1.

Date: June 29, 2021

City and state: St. Louis, MO


 Judge's signature

Honorable Nannette A. Baker, U.S. Magistrate Judge

Printed name and title

AUSA: Matthew Drake

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

| | | |
|--|---|----------------------|
| IN THE MATTER OF THE SEARCH OF |) | |
| THE PREMISES LOCATED AT: 507 E |) | No. 4:21 MJ 5163 NAB |
| Missouri St, Kirksville, MO 63501 located in |) | FILED UNDER SEAL |
| the Eastern District of Missouri. |) | |
| |) | |

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Thomas Putting, a Special Agent with Homeland Security Investigations, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 507 E Missouri St, Kirksville, MO 63501 which is located in the Eastern District of Missouri (hereinafter the "SUBJECT PREMISES"), further described in Attachment A, for the things described in Attachment B.

2. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations ("HSI"), since March 2019, and am currently assigned to the HSI office in Saint Louis, Missouri. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18

U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(1) (distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography) (hereinafter the “SUBJECT OFFENSES”) are presently located at the location to be searched, and within computer(s) and related peripherals, computer hardware and media, and wireless telephones found at that location.

LOCATION TO BE SEARCHED

5. The location to be searched (the “SUBJECT PREMISES”) is a single-story single-family residence which is located on Missouri Street. The residence has white and bluish siding and a black shingled roof. There is “507” in black numbering to the left of the front door area and “507” on the mailbox attached to the right of the front door area. A photograph of the home is attached to this Affidavit and labeled as “Attachment A”.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. The “BitTorrent Network” is a very popular and publicly available peer-to-peer file sharing network. Most computers that are part of this network are referred to as “peers”. Like most sharing networks, it is decentralized, as there is not any central hub for the network; also, files are not stored on a central server but are exchanged directly between users based on the peer-to-peer principle of the BitTorrent network protocol. In order to share a file or a set of files on the BitTorrent network, a “Torrent” file needs to be created by the user that initially wants to share the file or set of files.

b. “Cache” refers to text, image and graphic files sent to and temporarily stored by a user’s computer from a web site accessed by the user in order to allow the user speedier access to and interaction with that web site.

c. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

d. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. “Child pornography,” as defined in 18 U.S.C. § 2256(8), includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where the production of the visual depiction involved the use of a minor engaged

in sexually explicit conduct, or the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

g. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that

creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. “Geo-located,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

j. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

k. A “hash value” is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

l. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

m. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP

addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

n. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

p. “Mobile application” or “chat application,” as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

q. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

t. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

u. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

v. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, sharing photos or videos, reading a book, or playing a game.

w. The term “Online Chat Room” is defined as the real time visual interface which displays messages and responses of participants who are using online chat. Chat rooms are usually devoted to specific topics such as US politics; however, there are a number of general chat rooms which are devoted to any issue the participants wish to bring up. Participants usually communicate by typing their contributions into a simple text box line by line. The primary use of a chat room is to share information via text with a group of other users. New technology has enabled the use of file sharing and webcams to be included in some programs and almost all Internet chat rooms, or messaging services allow users to display and/or send pictures.

x. The term “Open Source” or “Open Source Software” is defined as software that makes available the software’s source code. This enables the software to be viewed and changed by a programmer.

y. A “Peer-to-Peer Network” is a sharing and delivery of user specified files among groups of people who are logged onto a file sharing network via the Internet; a type of Internet network that allows users with the same, or similar, program to connect with each other and access files on one another’s hard drive.

z. A “SHA1” (also referred to as “SHA-1”) is an algorithm that uses the Secure Hash Algorithm (SHA), developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard. Basically, the SHA1 is an algorithm for computing a condensed representation of a message or data file like a fingerprint.

aa. A “Torrent” is typically a small file that describes the file(s) that are being shared, which may include information on how to locate the file(s) on the BitTorrent network. A typical BitTorrent client will have the ability to create a “Torrent” file. It is important to note that the “Torrent” file does not contain the actual file(s) being shared, but information about the file(s) described in the “Torrent”, such as the name(s) of the file(s) being referenced in the “Torrent” and the “info hash” of the “Torrent”. The “info hash” is a SHA-1 hash value of the set of data describing the file(s) referenced in the “Torrent”, which include the SHA-1 hash value of each file piece, the file size, and the file name(s). The “info hash” of each “Torrent” uniquely identifies the

“Torrent” file on the BitTorrent network. The “Torrent” file may also contain information on how to locate file(s) referenced in the “Torrent” by identifying “Trackers”.

bb. “Trackers” are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the files(s) referenced in the “Torrent” file. A “Tracker” is only a pointer to peers/clients on the network who may be sharing part, or all of the file(s) referenced in the “Torrent”. It is important to note that the “Trackers” do not actually have the files(s) and are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. Typical client-side software that can be installed on a subject’s machine to share files over this network include BitTorrent, uTorrent, Vuze, and other client programs. Once installed on a computer system, a user can search the network for files. The BitTorrent network supports searching of files by the user’s use of keyword searchers within the BitTorrent network client itself or on websites hosting “Torrents”. Once a “Torrent” file is located that meets the keyword search criteria, the user will download the “Torrent” file to their computer. The BitTorrent network client will then process that “Torrent” file in order to find “Trackers” or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the files(s) referenced in the “Torrent” file.

cc. The term “web site” consists of text pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol.

dd. “Wireless telephone or mobile telephone, or cellular telephone or cell phone or smartphone” as used herein means a handheld wireless device used for voice and data

communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

COMPUTERS AND CHILD PORNOGRAPHY

7. From my own training and experience in the area of Internet-based child exploitation investigations, and through consultation with other knowledgeable law enforcement officials, I know the following to be true. Computers connected to the Internet identify each other by an Internet Protocol (“IP”) address. An IP address can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead a law enforcement officer to a particular Internet service company and that company can typically identify the account that uses or used the address to access the Internet.

8. The information contained in this section is based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions.

9. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-based/ subscription-based Web sites to conduct business, allowing them to remain relatively anonymous. Child pornography is also traded through chat rooms and file sharing software.

a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography

can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

b. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as America Online (“AOL”) and Microsoft, which allow subscribers to dial a local number and connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

c. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) Web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and

verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the Web sites and images accessed by the recipient.

d. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 40 gigabytes or more are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

BITTORRENT AND CHILD PORNOGRAPHY

10. A significant aspect of the Internet is peer to peer (P2P) file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the information is first deposited before

it is distributed. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from one folder to another to stop the distribution across the Internet. Further, once a file or files are placed in a shared folder its distribution is dependent only on the machine being turned on and connected to the Internet.

11. BitTorrent is one type of P2P file sharing software. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a “torrent” file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their “infohash”, which uniquely identifies the torrent based on the file(s) associated with the torrent file. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

12. One of the advantages of P2P file sharing is that multiple files may be downloaded at the same time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading a movie file may actually receive parts of the movie from multiple computers. The advantage of this is that it speeds up the time it

takes to download the file. Individuals downloading content on the BitTorrent file sharing network may download the content from a single sharing computer or may download pieces of content from multiple sharing computers. Although downloading content from multiple computers is preferred by this file sharing network, it accounts for users to also be able to download from a single sharing computer (an example being when only one source for the file is currently online).

13. The BitTorrent Network bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the digital fingerprinting of data. Once you check a file or files with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

14. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address can either be an IP version 4 address or an IP version 6 address. An IP version 4 address is expressed as four numbers separated by decimal points, is unique to a particular computing device during an online session. The IP address provides a unique location making it possible for data to be transferred between computers. IP version 6 address is alpha/numeric and is a 128-bit value expressed in hexadecimal. This value has 8 segments which is separated by a colon.

15. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) can assign a different unique number to a computer when it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

16. As a result of my consultations with other law enforcement officers, both federal and state, who have considerable experience investigating the sexual exploitation of children, and my own experience, your affiant has learned about the individuals engaged in child exploitation activities and about the computer technology available to, and utilized by, those individuals. Your affiant has learned that individuals engaged in the production, procurement, trade, and/or transmission of child pornography through the United States mail, computer or other interstate conveyance commonly:

- a. Receive sexual gratification and satisfaction from actual physical contact with children and from fantasy that may be stimulated by producing and viewing children engaged in sexual activity or in sexually suggestive poses;
- b. own and operate photographic production and reproduction equipment. This equipment is often digital cameras which include both cameras which take still images and movie files;
- c. collect sexually explicit or suggestive materials of adults and/or children consisting of photographs, magazines, motion pictures, videotapes, books, slides, computer images, drawings or other visual media for their own sexual arousal and gratification, and in some instances, to lower the inhibitions of children they are attempting to seduce, and/or to arouse and to demonstrate their desired sexual acts to their selected partners;
- d. often do not dispose of their collection of sexually explicit material, in the event that the material is discarded or lost due to computer malfunction, these individuals often replenish their supply of child pornography very quickly;

- e. correspond with individuals who share their same interest in child pornography, and maintain their names, addresses, telephone numbers, and other identifying information in lists, telephone books, address books, scraps of paper, or on computer disks;
- f. obtain, collect and maintain photographs of children they are or have been involved with, which may depict children fully clothed, in various states of undress, totally nude, or in various activities, which are often held for lengthy periods of time;
- g. commonly collect items which could be any material relating to children that serve a sexual purpose for a given individual, these items as used herein, have been termed “child erotica.” Some of the more common types of “child erotica” include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;
- h. often do not discard the child exploitation material but collect it over a long period of time and maintain this material in the privacy of their homes. Sometimes, individuals using peer to peer software will engage in a routine where they may delete their child exploitation material after they have viewed it a number of times and then after the deletion occurs the individual will replenish their supply via their peer to peer connection when they desire more images to satisfy their sexual interest in children. This procurement and purging cycle results in evidence of their current child pornography images being easily located on their computer as well as evidence of their deleted material still

remaining on their computer which can be recovered by a forensic computer examiner.

PROBABLE CAUSE

17. On or about May 10, 2021, your affiant was contacted by a Homeland Security Investigations Special Agent in Kansas City, Missouri, who was conducting an undercover investigation on the BitTorrent Peer-to-Peer (P2P) file sharing network. On May 2, 2021, a connection was made between the agent's investigative computer and a computer device running BitTorrent software with the assigned IP Address 107.192.241.236. This IP address reported that it had two (2) completed files which is referenced by torrent with infohash 8b9942f242646929f0e50d6df08b126791f5998f.

18. The agent was able to successfully download the two (2) files. The agent transferred the files to your affiant. Your affiant reviewed the files and found one (1) image of child pornography and one (1) video of child pornography. The image of child pornography consisted of multiple screen shots of the video of child pornography in the same file. A description of the video is as follows:

- a. "[JulyJailbait.nl] – [jjclubumn7vkhyuw.onion] – Stars & Stripes (New studio) – video 00103" – this is a graphic video file, approximately ten (10) minutes and twenty-three (23) seconds in length, that depicts, in part, a prepubescent and postpubescent female engaging in sexual acts, including: prepubescent female inserting a finger into her exposed anus; postpubescent female rubbing the clothed and exposed vagina of prepubescent female; postpubescent female

inserting a finger into exposed anus of prepubescent female; postpubescent female licking exposed vagina of prepubescent female.

19. A query of the American Registry for Internet Numbers (“ARIN”) online database revealed that the IP address 107.192.241.236 is registered to AT&T Inc.

20. On or about May 5, 2021, an HSI administrative summons (Summons number ICE-HSI-KC-2021-00759) was issued to AT&T, Inc., for the assigned subscriber to IP address 107.192.241.236 used on May 1, 2020, 05:00:00 UTC to May 5, 2021, 05:00:00 UTC.

21. On or about May 7, 2021, AT&T Inc, responded to HSI administrative summons HSI-KC-2021-00759. According to records, that IP address resolved to the SUBJECT PREMISES. Specifically, the records showed:

| | |
|-------------------|---|
| Name: | Daniel SPURGEON |
| Address: | 507 E Missouri St, Kirksville, MO 63501 |
| Phone Number: | 660-349-8634 |
| Account Number: | 159595249 |
| Email Address: | FIREDRAGON72580@yahoo.com |
| IP Address: | 107.192.241.236 |
| Account Creation: | 03/13/2017 |

22. A check with public database systems on or about May 12, 2021, revealed that an individual named Daniel SPURGEON, with a Date of Birth of July 25, 1980, resides at the SUBJECT PREMISES.

23. On May 19, 2021, your affiant conducted surveillance of the SUBJECT PREMISES and observed a green Ford F150 with a red driver side door parked in front of the residence. The vehicle was bearing Missouri license plate ODEC14. A check with a public database system revealed the vehicle was registered to SPURGEON.

24. On March 15, 2021, representatives of the City of Kirksville indicated that water service for the SUBJECT PREMISES is current and that the responsible party is Daniel SPURGEON.

25. On May 19, 2021, your affiant used his government-issued iPhone in an effort to gain additional information regarding any potential wireless networks at the SUBJECT PREMISES. Positioned approximately ten (10) yards from the SUBJECT PREMISES, your affiant noted that there were multiple wireless networks in the area, but all of them were secured. Accordingly, to use any of them to access the Internet, a user would likely have to know the encryption key or password for that particular network. Based on the signal strength of the wireless networks, as well as my training and experience and information relayed to me by agents, your affiant believes that the wireless router at the SUBJECT PREMISES, is likely generating a secured wireless network. As explained above, I know, from my training and experience and information relayed to me by agents, that wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime.

**CHARACTERISTICS OF INDIVIDUALS WHO RECEIVE AND COLLECT IMAGES
OF CHILD PORNOGRAPHY**

26. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals

involved in the receipt and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Collectors of child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the collector to view the collection, which is valued highly.

e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Collectors of child pornography prefer to have continuous access to their collection of child pornography. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

27. Based upon the conduct of individuals involved in the collection of child pornography set forth above, namely, that they tend to maintain their collections at a secure, private location for long periods of time, there is probable cause to believe that evidence of the offenses of receiving and possessing child pornography is currently located at the premises described previously herein, known as, and the computers and computer media located therein.

SEIZURE OF EQUIPMENT AND DATA

28. Based upon my knowledge, training and experience, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

a. The volume of evidence. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process may take weeks or months, depending on the volume of data stored and it would be impractical to attempt this kind of data analysis on-site.

b. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even “hidden”, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

29. Due to the volume of the data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under appropriate circumstances, some types of computer equipment can be more readily

analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus subject to immediate seizure as such-- or whether it serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readily, quickly, and thus less intrusively analyzed off site, with due consideration given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

30. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - - for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are

automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

31. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel with whom I have spoken, I am aware that searches and seizures of evidence from computers taken from the subject premises commonly require agents to seize most or all of a computer system’s input/output peripheral devices, in order for a qualified computer expert to accurately retrieve the system’s data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the subject premises, and in order to fully retrieve data from a computer system, investigators must seize all magnetic storage devices as well as the central processing units (CPU) and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, such materials and/or equipment will be returned within a reasonable time.

32. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called “wireless

routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

COMPUTER EXAMINATION METHODOLOGY TO BE EMPLOYED

33. The examination procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other examination procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal

activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BIOMETRIC ACCESS

34. Through my training and experience, as well as from information found in publicly available materials published by device manufacturers, I am informed of the information contained in the following paragraphs concerning biometric features of electronic devices. Many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

35. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. The

fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

36. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. Apple's facial recognition feature is referred to as Face ID and it allows a user to unlock the iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of the user's face. Face ID confirms attention by detecting the direction of the user's gaze, then uses neural networks for matching and anti-spoofing so the user can unlock the phone with a glance. Face ID automatically adapts to changes in the user's appearance, and carefully safeguards the privacy and security of the user's biometric data. Similarly, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

37. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

38. Beginning with the release of Apple’s iOS 8 operating system in September 2014, Apple no longer has a key to decrypt these devices. Thus, even with a properly authorized search warrant to gain access to the content of an iOS device, there is no feasible way for the government to search the device.

39. Users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

40. As discussed in this Affidavit, there is reason to believe that one or more digital electronic devices, (Device(s)), will be found during the search. The passcode or password that would unlock any Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data

contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

41. I am also informed through my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Further, Touch ID will not allow access if the device has been turned off or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

42. A person who is in possession of a Device or has the Device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via biometric data, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty

who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, during the execution of the search of the Premises described in Attachment A, law enforcement personnel request permission to obtain from persons located on the SUBJECT PREMISES at the time of execution of the warrant, the display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Devices requiring such biometric access subject to seizure pursuant to this warrant, that is, including pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:


- a. any Device(s) found at the SUBJECT PREMISES for which law enforcement can reasonably identify the user of the Device(s) without the use of biometrics; and
- b. Device(s) are limited to those which are capable of containing, and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments.

CONCLUSION

43. Based on the above information, there is probable cause to believe that the SUBJECT OFFENSES have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES described in Attachment A, and any computers, computer media, or wireless telephones therein, and more fully described herein. Your Affiant requests

authority to seize such material, specifically, that the Court issue a search warrant for these premises and all computers, computer hardware and media, and wireless telephones therein.

I state under the penalty of perjury that the foregoing is true and correct.



THOMAS PUTTING
Special Agent
Homeland Security Investigations

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on _____ June 29, 2021.



HONORABLE NANNETTE A. BAKER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The location to be searched (the “SUBJECT PREMISES”) is a single-story single-family residence which is located on Missouri Street. The residence has white and bluish siding and a black shingled roof. There is “507” in black numbering to the left of the front door area and “507” on the mailbox attached to the right of the front door area.



ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

All records, items, and information constituting evidence, instrumentalities and contraband concerning the violations of 18 U.S.C. §§ 2252A(a)(1) (distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography), including as follows:

2. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the distribution, receipt or storage of the same, including but not limited to:

a. Any computer, cell phone, computer system and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, cell phones, computer compact disks, CD-ROMS, DVD, and other memory storage devices) (hereinafter referred to collectively as Devices);

b. peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and

c. any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

3. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

4. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to the possession or production of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received.

5. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

6. Documents and records regarding the ownership and/or possession of the SUBJECT PREMISES.

7. During the course of the search, photographs of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items therein.

8. During the execution of the search of the Premises described in Attachment A, law enforcement personnel are also specifically authorized to obtain from persons located on the SUBJECT PREMISES at the time of execution of the warrant, the display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Devices requiring such biometric access subject to seizure pursuant to this warrant, that is, including pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any Device(s) found at the SUBJECT PREMISES for which law enforcement can reasonably identify the user of the Device(s) without the use of biometrics; and

b. Device(s) are limited to those which are capable of containing, and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments.

The proposed warrant does not authorize (nor does it prohibit) law enforcement to request that the aforementioned person(s) state or otherwise provide the password or any other means that may be used to unlock or access the Device(s). Moreover, the proposed warrant does not authorize (nor does it prohibit) law enforcement to ask the aforementioned person(s) to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s).